IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: **DELLOW ET AL.**	)
	) Examiner: **ALMEDIA, DEVIN E**
Serial No. **10/817,148**	)
Confirmation No. **1198**	) Art Unit: **2432**
Filing Date: **APRIL 2, 2004**	)
	) Attorney docket:
For: **MEMORY SECURITY DEVICE FOR FLEXIBLE SOFTWARE ENVIRONMENT**	) **52840**

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Responsive to the final Office Action of November 4, 2008, and in connection with the Notice of Appeal filed concurrently herewith, please consider the remarks set out below.

REMARKS

Based upon the arguments presented below, Applicants respectfully request the Pre-Appeal Brief Conference Panel reconsider and withdraw the Examiner's rejections of the claims. As detailed herein, Applicants submit that the Examiner's proposed combination of the diagnostic tool of Warren and the secure code computing device of Goffin et al. fails to disclose the claimed invention and lacks sufficient rationale for combination.

The Examiner rejected independent Claims 1, 19, 25, and 31 over Warren in view of Goffin et al. Warren discloses an integrated circuit comprising a CPU, a bus coupled to the CPU, a memory coupled to the bus, a breakpoint range unit storing first and second breakpoint addresses, and a logic controller coupled to the breakpoint range unit. The breakpoint range unit compares the instruction address currently being processed by the CPU. If the current instruction address falls within the first and second breakpoint addresses, the breakpoint range unit generates a breakpoint signal, which is received by the logic controller. Upon receipt of the

breakpoint signal, the logic controller interrupts the CPU, thereby enabling diagnostic tests on the CPU. (Col. 2, lines 25-47).

The Examiner correctly notes that Warren fails to disclose the verifier processor continually processing the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, as recited, for example, in independent Claim 1. The Examiner looks to Goffin et al. to supply this deficiency of Warren.

Goffin et al. discloses a first embodiment of a computing device that includes a master processor 101, a master memory unit 103 coupled to the master processor via a memory bus 104, and a secure processor 102 also coupled to the memory via the memory bus. *See* Figure 1, reproduced below. The code is first downloaded by the master processor and stored in the master memory unit for subsequent authentication by the secure processor. (Page 10, line 32 through Page 12, line 12). The secure processor receives the code via the memory bus. (Page 12, lines 1-3). If the code is not authentic, the secure processor can erase or disable the adulterated memory blocks or disable the entire computing device. (Page 13, lines 12-18). The secure processor may periodically sweep code stored in the master memory unit for re-authentication. (Page 14, lines 5-16).

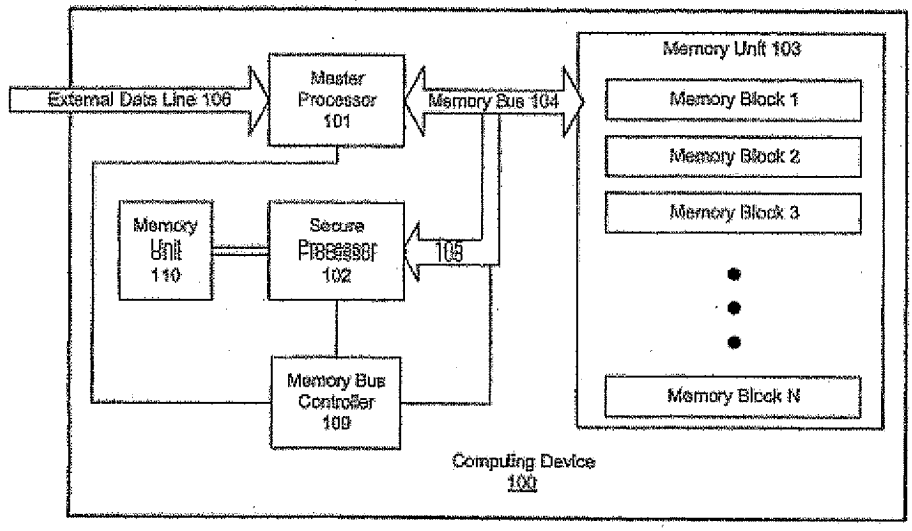


Figure 1 of Goffin et al.

In an alternative embodiment, the code is initially received by the secure processor rather than the master processor. (Page 12, lines 13-15). In this embodiment, the secure processor receives the code and stores it in an interim memory before long-term storage of authenticated code in the master memory unit. (Page 12, lines 13-23). Goffin et al. does not disclose how the secure processor receives the code directly.

Applicants submit that Goffin et al. fails to disclose the verifier processor receiving the application code via the internal bus, and the processor executing the application code from the memory independently of the verifier processor, as recited in independent Claim 1. In the first embodiment, i.e. where the master processor first receives code and stores it for subsequent authentication, the verification routine is not independent from the master processor since it first receives the code for storage. In the second embodiment, i.e. where the secure processor receives the code first, the code is not received via the memory bus, as in the first embodiment. In other words, Goffin et al. fails to disclose both the verifier processor receiving the application

code via the internal bus, and the processor executing the application code from the memory independently of the verifier processor, as recited in independent Claim 1. For this reason alone, independent Claim 1 is patentable over the prior art.

Moreover, Applicants submit that the person of ordinary skill in the art would not be motivated to combine two disparate embodiments of Goffin et al. *Cf. Boston Sci. Scimed, Inc. v. Cordis Corp.*, 2009 U.S. App. LEXIS 588 (Fed. Cir. 2009) and *GNB Battery Techs. v. Exide Corp.*, 38 U.S.P.Q.2D 1506 (Fed. Cir. 1996). Indeed the person of ordinary skill in the art would be taught away from such a selective combination since the code is typically received by a processor to be addressed and routed via the memory bus, i.e. the code is received by either the master processor or the secure processor and not both as suggested by the Examiner.

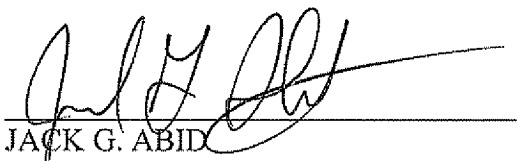
Applicants also note that Goffin et al. fails to disclose the verifier processor continually processing the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, as recited by independent Claim 1, for example. Differently, in Goffin et al., the authentication of the code by the secure processor is sequentially performed before any execution by the master processor. Moreover, even during re-authentication, the secure processor gives way to the master processor's use of the memory bus, for example, when the master processor is accessing code for execution. (Page 14, line 17 through Page 15, line 8). Therefore, for this additional reason, independent Claim 1 is patentable over the prior art.

The Examiner's stated motivation to combine Warren with Goffin et al. is to increase security of the system. Furthermore, Applicants submit that the Examiner's combination is improper because the prior art references teach away from such a selective combination. More particularly, Warren discloses an integrated circuit for diagnostic procedures, i.e. interrupting normal operation of the CPU to allow diagnostic procedures to be implemented. (Col. 1, lines 5-8). Differently, Goffin et al. discloses a computing device that provides for secure downloading

of software. (Page 1, lines 8-25). Given that Warren deals with diagnostics and not security, Applicants submit that the person of ordinary skill in the art would be taught away from the Examiner's proposed selective combination.

Accordingly, because of the above noted critical deficiencies of the prior art, independent Claim 1 is patentable over the prior art. Independent Claims 19, 25, and 31 are similar to Claim 1 and are patentable for similar reasoning. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

Respectfully submitted,



JACK G. ABID
Reg. No. 58,237
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Orlando, Florida 32802
407-841-2330
Attorney for Applicants